AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for operating a key distribution center (KDC) that provides keys to facilitate secure communications between clients and servers across a computer network, wherein the KDC operates without having to store long-term server secrets, comprising:

receiving a communication from a server that is authenticated at the KDC;

wherein the communication includes a temporary secret key to be used in communications with the server for a limited time period, and wherein the temporary secret key is shared between the server and the KDC; and

storing the temporary secret key in a database at the KDC, so that the temporary secret key can be subsequently used to facilitate one or more communications between a client and the server, wherein the temporary secret key is encrypted with a public key belonging to the KDC, so that the temporary secret key can only be decrypted using a private key belonging to the KDC;

wherein the temporary secret key is a short-term secret which becomes invalid after a short time period~~,~~; and wherein a new temporary secret key is ~~subsequently~~ generated in response to a request from the KDC for a new temporary secret key to replace the invalid temporary secret key, thereby avoiding the overhead of periodically establishing a new temporary secret key. ~~which reduces the vulnerability of the KDC~~.

2. (Original) The method of claim 1, wherein upon subsequently receiving a request from the client at the KDC to communicate with the server, the method further comprises facilitating communications between the client and the server by:

producing a session key to be used in communications between the client and server;

creating a ticket to the server by encrypting an identifier for the client and the session key with the temporary secret key for the server; and

assembling a message that includes the identifier for the server, the session key and the ticket to the server; and

sending the message to the client in a secure manner; and

allowing the client to forward the ticket to the server in order to initiate communications between the client and the server.

3. (Original) The method of claim 2, wherein upon receiving the ticket from the client at the server, the method further comprises:

decrypting the ticket at the server using the temporary secret key to restore the session key and the identifier for the client; and

using the session key at the server to protect subsequent communications between the server and the client.

4. (Original) The method of claim 2, wherein assembling the message involves including an expiration time for the session key in the message.

5. (Original) The method of claim 2, wherein allowing the client to forward the ticket to the server includes allowing the client to forward an identifier for the temporary secret key to the server, so that the server can know which temporary secret key to use in decrypting the ticket.

6. (Original) The method of claim 2, wherein sending the message to the client in the secure manner involves encrypting the message with a second session key that was previously communicated to the client by the KDC.

7. (Original) The method of claim 2, further comprising alternatively creating the ticket to the server by encrypting the identifier for the client and the session key with one of:

a public key for the server; and

a secret key for the server previously agreed upon between the server and the KDC and stored at the KDC.

8. (Original) The method of claim 1, wherein receiving the communication from the server involves authenticating the server.

9. (Original) The method of claim 8, wherein authenticating the server involves using authentication information pertaining to the server, the authentication information including a certificate chain from a trust anchor to the server, and including a server public key that is associated with a server private key to form a public key-private key pair associated with the server.

10. (Original) The method of claim 8, wherein authenticating the server involves authenticating the server without having prior configuration information pertaining to the server at the KDC.

11. (Original) The method of claim 8, wherein authenticating the server includes using a server public key that is stored locally in the KDC.

12 (Canceled).

13. (Original) The method of claim 1, wherein the communication is signed with a server private key so that the KDC can use a corresponding server public key to verify that the communication was sent by the server.

14. (Original) The method of claim 1, wherein the communication is received in response to a request being sent by the KDC to the server indicating that the temporary secret key is needed from the server.

15. (Original) The method of claim 1, further comprising communicating information to the server that enables the server to authenticate the KDC.

16. (Original) The method of claim 1, wherein the KDC operates in accordance with the Kerberos standard.

17. (Original) The method of claim 1, wherein the communication received from the server additionally includes an identifier for the server.

18. (Original) The method of claim 1, further comprising propagating the temporary secret key to multiple KDCs.

19. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for operating a key distribution center (KDC) that provides keys to facilitate secure communications between clients and servers across a computer network, wherein the KDC operates without having to store long-term server secrets, the method comprising:

receiving a communication from a server that is authenticated at the KDC;

wherein the communication includes a temporary secret key to be used in communications with the server for a limited time period, and wherein the temporary secret key is shared between the server and the KDC; and

storing the temporary secret key in a database at the KDC, so that the temporary secret key can be subsequently used to facilitate one or more communications between a client and the server, wherein the temporary secret key is encrypted with a public key belonging to the KDC, so that the temporary secret key can only be decrypted using a private key belonging to the KDC;

wherein the temporary secret key is a short-term secret which becomes invalid after a short time period~~,~~; and wherein a new temporary secret key is ~~subsequently~~ generated in response to a request from the KDC for a new temporary secret key to replace the invalid temporary secret key, thereby avoiding the overhead of periodically establishing a new temporary secret key. ~~which reduces the vulnerability of the KDC.~~

20. (Original) The computer-readable storage medium of claim 19, wherein upon subsequently receiving a request from the client at the KDC to communicate with the server, the method further comprises facilitating communications between the client and the server by:

producing a session key to be used in communications between the client and server;

creating a ticket to the server by encrypting an identifier for the client and the session key with the temporary secret key for the server; and

assembling a message that includes the identifier for the server, the session key and the ticket to the server; and

sending the message to the client in a secure manner; and

allowing the client to forward the ticket to the server in order to initiate communications between the client and the server.

21. (Original) The computer-readable storage medium of claim 20, wherein upon receiving the ticket from the client at the server, the method further comprises:

decrypting the ticket at the server using the temporary secret key to restore the session key and the identifier for the client; and

using the session key at the server to protect subsequent communications between the server and the client.

22. (Original) The computer-readable storage medium of claim 20, wherein assembling the message involves including an expiration time for the session key in the message.

23. (Original) The computer-readable storage medium of claim 20, wherein allowing the client to forward the ticket to the server includes allowing the client to forward an identifier for the temporary secret key to the server, so that the server can know which temporary secret key to use in decrypting the ticket.

24. (Original) The computer-readable storage medium of claim 20, wherein sending the message to the client in the secure manner involves encrypting the message with a second session key that was previously communicated to the client by the KDC.

25. (Original) The computer-readable storage medium of claim 20, wherein the method further comprises alternatively creating the ticket to the server by encrypting the identifier for the client and the session key with one of:

a public key for the server; and

a secret key for the server previously agreed upon between the server and the KDC and stored at the KDC.

26. (Original) The computer-readable storage medium of claim 19, wherein receiving the communication from the server involves authenticating the server.

27. (Original) The computer-readable storage medium of claim 26, wherein authenticating the server involves using authentication information pertaining to the server, the authentication information including a certificate chain from a trust anchor to the server, and including a server public key that is associated with a server private key to form a public key-private key pair associated with the server.

28. (Original) The computer-readable storage medium of claim 26, wherein authenticating the server involves authenticating the server without having prior configuration information pertaining to the server at the KDC.

29. (Original) The computer-readable storage medium of claim 26, wherein authenticating the server includes using a server public key that is stored locally in the KDC.

30 (Canceled).

31. (Original) The computer-readable storage medium of claim 19, wherein the communication is signed with a server private key so that the KDC can use a corresponding server public key to verify that the communication was sent by the server.

32. (Original) The computer-readable storage medium of claim 19, wherein the communication is received in response to a request being sent by the

KDC to the server indicating that the temporary secret key is needed from the server.

33. (Original) The computer-readable storage medium of claim 19, wherein the method further comprises communicating information to the server that enables the server to authenticate the KDC.

34. (Original) The computer-readable storage medium of claim 19, wherein the KDC operates in accordance with the Kerberos standard.

35. (Original) The computer-readable storage medium of claim 19, wherein the communication received from the server additionally includes an identifier for the server.

36. (Original) The computer-readable storage medium of claim 19, wherein the method further comprises propagating the temporary secret key to multiple KDCs.

37. (Currently amended) An apparatus that provides keys to facilitate secure communications between clients and servers across a computer network, wherein the apparatus operates without having to store long-term server secrets, comprising:

a key distribution center (KDC);

a receiving mechanism within the KDC that is configured to receive a communication from a server;

wherein the communication includes a temporary secret key to be used in communications with the server for a limited time period, and wherein the temporary secret key is shared between the server and the KDC; and

a storage mechanism within the KDC that is configured to store the temporary secret key in a database at the KDC, so that the temporary secret key can be subsequently used to facilitate one or more communications between a client and the server, wherein the temporary secret key is encrypted with a public key belonging to the KDC, so that the temporary secret key can only be decrypted using a private key belonging to the KDC;

wherein the temporary secret key is a short-term secret which becomes invalid after a short time period~~,~~; and wherein a new temporary secret key is ~~subsequently~~ generated in response to a request from the KDC for a new temporary secret key to replace the invalid temporary secret key, thereby avoiding the overhead of periodically establishing a new temporary secret key. ~~which reduces the vulnerability of the KDC.~~

38. (Original) The apparatus of claim 37, further comprising a communication facilitation mechanism within the KDC, wherein upon receiving a request from the client to communicate with the server, the communication facilitation mechanism is configured to:

produce a session key to be used in communications between the client and server;

create a ticket to the server by encrypting an identifier for the client and the session key with the temporary secret key for the server;

assemble a message that includes the identifier for the server, the session key and the ticket to the server;

send the message to the client in a secure manner; and to

allow the client to forward the ticket to the server in order to initiate communications between the client and the server.

39. (Original) The apparatus of claim 38, further comprising a mechanism within the server that is configured to:

decrypt the ticket received from the client using the temporary secret key to restore the session key and the identifier for the client; and to

use the session key to protect subsequent communications between the server and the client.

40. (Original) The apparatus of claim 38, wherein the communication facilitation mechanism is configured to include an expiration time for the session key in the message.

41. (Original) The apparatus of claim 38, wherein the client is configured to additionally forward an identifier for the temporary secret key to the server, so that the server can know which temporary secret key to use in decrypting the ticket.

42. (Original) The apparatus of claim 38, wherein in sending the message to the client in the secure manner, the communication facilitation mechanism is configured to encrypt the message with a second session key that was previously communicated to the client by the KDC.

43. (Original) The apparatus of claim 38, wherein the communication facilitation mechanism is configured to alternatively create the ticket to the server by encrypting the identifier for the client and the session key with one of:

a public key for the server; and

a secret key for the server previously agreed upon between the server and the KDC and stored at the KDC.

44. (Original) The computer-readable storage medium of claim 37, further comprising an authentication mechanism that is configured to authenticate the server.

45. (Original) The apparatus of claim 44, wherein in authenticating the server, the authentication mechanism is configured to use authentication information pertaining to the server, the authentication information including a certificate chain from a trust anchor to the server, and including a server public key that is associated with a server private key to form a public key-private key pair associated with the server.

46. (Original) The apparatus of claim 44, wherein in authenticating the server the authentication mechanism is configured to operate without having prior configuration information pertaining to the server at the KDC.

47. (Original) The apparatus of claim 44, wherein in authenticating the server, the authentication mechanism is configured to use a server public key that is stored locally in the KDC.

48 (Canceled).

49. (Original) The apparatus of claim 37, wherein the communication is signed with a server private key so that the KDC can use a corresponding server public key to verify that the communication was sent by the server.

50. (Original) The apparatus of claim 37, further comprising a requesting mechanism within the KDC that is configured to send a request to the server indicating that the temporary secret key is needed from the server.

51. (Original) The apparatus of claim 37, further comprising a sending mechanism that is configured to send information to the server that enables the server to authenticate the KDC.

52. (Original) The apparatus of claim 37, wherein the KDC is configured to operate in accordance with the Kerberos standard.

53. (Original) The apparatus of claim 37, wherein the communication received from the server additionally includes an identifier for the server.

54. (Original) The apparatus of claim 37, wherein the storage mechanism is additionally configured to communicate the temporary secret key to multiple KDCs.